修 士 論 文 の 和 文 要 旨

研究科・専攻	大学院　電気通信学研究科　人間コミュニケーション学専攻　博士前期課程		
氏　　名	金子　聡	学籍番号	0636007
論 文 題 目	暗号学的安全性モデルに基づく電子透かしアルゴリズムの評価と改良		

要　　旨

デジタルコンテンツの不正コピー対策として，コンテンツに配布先氏名などの情報を埋め込む電子透かしが注目されている．従来の電子透かしは情報の埋め込みおよび検出手順といったアルゴリズムを公開しないことを前提にしていた．しかし，電子透かしの高度化，普及のためにはアルゴリズムを公開した上で，第三者の評価を受け，誰もが利用可能とする必要がある．そこで，アルゴリズムを公開しても安全な電子透かし方式を検討した．

まず，暗号とのアナロジーに基づく電子透かしアルゴリズムの安全性分析方法を提案した．具体的には，暗号と電子透かしの対応付けを行い，暗号分析学に基づき，攻撃者の目的，能力，安全性の評価基準によって電子透かしへの攻撃を分類した，この分析方法を用いて，アルゴリズム公開時における従来の電子透かし方式を評価した結果，分類した全 12 ケースにおいて情報量的安全性が成立しないこと，全ケースのうち 6 ケースにおいて計算量的安全性が成立しないこと，他の 6 ケースにおいて計算量的安全性が成立しない可能性があることを示した．さらに，分析に基づき，暗号を組み込んだ方式と誤り検知符号を組み込んだ方式を提案した．提案方式により，電子透かしの安全性を暗号の安全性に帰着させることができた．